Agrégation externe de Mathématiques

session 1978

Mathématiques générales

Enoncé

Visitez le site Megamaths : http ://megamaths.perso.neuf.fr/

(Agrégation externe 1978) Dans tout le problème, ω désigne un entier pair strictement positif, Ω représente un ensemble de cardinal ω, et $\mathcal{P}(\Omega)$ représente l'ensemble des parties de Ω. Le cardinal d'un ensemble fini E est noté $|E|$, et la classe d'un entier n modulo 2 est noté $\overline{n}$. La notation $\mathbb{Z}[X,Y]$ représente l'anneau des polynômes à deux indéterminées et à coefficients dans $\mathbb{Z}$. Si $m \in \mathbb{N}^*$, la notation $\mathbb{N}_m$ représente l'ensemble $\{1, 2, ..., m\}$.

Les notations et certains résultats de la partie I seront utilisés dans les parties II.B et III.B. Les parties II et III sont indépendantes l'une de l'autre.

Partie I

I.A. Généralités

I.A.1. Vérifier que $\mathcal{P}(\Omega)$ muni de la loi « différence symétrique » définie par $(x, y) \mapsto x+y = (x \cup y) \setminus (x \cap y)$ est un groupe abélien.

I.A.2. Démontrer que $\mathcal{P}(\Omega)$ peut être muni d'une structure d'espace vectoriel sur le corps à deux éléments $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ pour la loi $+$ définie en **I.A.1**. Grâce à quelle propriété particulière de cette loi de groupe cela est-il possible ?

I.A.3. Quelle est la dimension de $\mathcal{P}(\Omega)$? Donner une base de cet espace.

I.A.4. Vérifier que l'application α de $\mathcal{P}(\Omega) \times \mathcal{P}(\Omega)$ dans $\mathbb{F}_2$ définie par :

$$\alpha(x, y) = \overline{|x \cap y|}$$

est une forme bilinéaire symétrique non dégénérée sur $\mathcal{P}(\Omega)$. Cette forme bilinéaire sera appelée "forme bilinéaire naturelle sur $\mathcal{P}(\Omega)$".

I.A.5. Soient $\mathcal{D}(\Omega)$ la droite vectorielle de $\mathcal{P}(\Omega)$ engendrée par Ω, et $\mathcal{H}(\Omega) = \mathcal{D}(\Omega)^{\perp}$ l'orthogonal de $\mathcal{D}(\Omega)$ pour la forme bilinéaire α. Décrire $\mathcal{H}(\Omega)$, et retrouver ainsi la formule :

$$\binom{\omega}{0} + \binom{\omega}{2} + ... + \binom{\omega}{2k} + ... + \binom{\omega}{\omega} = 2^{\omega-1}.$$

Quel est le noyau de la restriction de la forme bilinéaire naturelle à $\mathcal{H}(\Omega)$?

I.B. Codes et Polynômes des Poids

Les sous-espaces vectoriels de $\mathcal{P}(\Omega)$ sont appelés les codes de $\mathcal{P}(\Omega)$. Si $\mathcal{C}$ est un code de $\mathcal{P}(\Omega)$, on désigne par $\mathcal{C}^{\perp}$ son orthogonal. Pour toute permutation s de Ω, on désigne par $\overline{s}$ l'endomorphisme de $\mathcal{P}(\Omega)$ définie par :

$$x \mapsto \overline{s}(x) = \{s(t) \;/\; t \in x\}.$$

On dit que deux codes $\mathcal{C}$ et $\mathcal{C}'$ de $\mathcal{P}(\Omega)$ sont isomorphes s'il existe une permutation s de Ω telle que $\overline{s}(\mathcal{C}) = \mathcal{C}'$.

I.B.1. Un code $\mathcal{C}$ est dit auto-orthogonal si $\mathcal{C} = \mathcal{C}^{\perp}$. Quelle est la dimension d'un code auto-orthogonal ? Démontrer que si $\mathcal{C}$ est auto-orthogonal on a $\mathcal{D}(\Omega) \subset \mathcal{C} \subset \mathcal{H}(\Omega)$.

Soit $\mathcal{C}$ un code de $\mathcal{P}(\Omega)$. On appelle polynôme des poids de $\mathcal{C}$ et on note $P_{\mathcal{C}}(X,Y)$ l'élément de $\mathbb{Z}[X,Y]$ défini par :

$$P_{\mathcal{C}}(X,Y) = \sum_{x \in \mathcal{C}} X^{|x|} Y^{\omega - |x|}.$$

I.B.2. On pose $\omega = 2m$ et $\Omega = \{t_1, t_2, ..., t_m, u_1, u_2, ..., u_m\}$. Construire un code auto-orthogonal dont le polynôme des poids est $P_{\omega}(X,Y) = \left(X^2 + Y^2\right)^m$. Soit $\Gamma(\Omega)$ l'ensemble

des codes auto-orthogonaux dont le polynôme des poids est $P_\omega(X,Y)$. Démontrer que deux éléments quelconques de $\Gamma(\Omega)$ sont isomorphes.

I.B.3. Dans cette question, on suppose que $\omega = 2m$ est un multiple de 4 et l'on note toujours :

$$\Omega = \{t_1, t_2, ..., t_m, u_1, u_2, ..., u_m\}.$$

On définit le code $\mathcal{B}_\omega$ engendré par :

$$\{t_1, t_2, ..., t_m\},\ \{u_1, u_2, ..., u_m\} \text{ et } \{t_h, t_j, u_h, u_j\} \text{ avec } h \neq j \text{ et } (h,j) \in \mathbb{N}_m^2.$$

I.B.3.a. On pose $\varepsilon_1 = \{t_1, t_2, ..., t_m\}$ et aussi pour tout $2 \leq h \leq m$, $\varepsilon_h = \{t_1, t_h, u_1, u_h\}$. Démontrer que la famille $(\varepsilon_h)_{1\leq h\leq m}$ est libre, puis que $\mathcal{B}_\omega$ est un code auto-orthogonal. En déduire que $(\varepsilon_h)_{1\leq h\leq m}$ est une base de $\mathcal{B}_\omega$.

I.B.3.b. Si μ est une partie non vide de $\mathbb{N}_m$, on pose :

$$\begin{cases} x_\mu = \{t_h \,/\, h \in \mu\} \cup \{u_h \,/\, h \in \mu\} \\ y_\mu = \{t_h \,/\, h \in \mu\} \cup \{u_h \,/\, h \in \mathbb{N}_m \backslash \mu\}. \end{cases}$$

On pose aussi $x_\varnothing = y_\varnothing = \varnothing$. On note $\mathcal{B}'_\omega$ la partie de $\mathcal{P}(\Omega)$ définie par :

$$\mathcal{B}'_\omega = \{x_\mu \,/\, \mu \subset \mathbb{N}_m \text{ et } |\mu| \text{ pair}\} \cup \{y_\mu \,/\, \mu \subset \mathbb{N}_m \text{ et } |\mu| \text{ pair}\}.$$

On admet les relations suivantes :

$$x_\mu = \sum_{\substack{h\in\mu \\ h\neq 1}} \varepsilon_h \quad \text{et} \quad y_\mu = \varepsilon_1 + x_{\mathbb{N}_m\backslash\mu}$$

qui prouvent l'inclusion $\mathcal{B}'_\omega \subset \mathcal{B}_\omega$. Démontrer que si $\mu \subset \mathbb{N}_m$ et $\mu' \subset \mathbb{N}_m$, alors $\overline{\mu} + \overline{\mu'} = \mu + \mu'$ et $\mu + \overline{\mu'} = \overline{\mu + \mu'}$. Démontrer ensuite que $\mathcal{B}'_\omega$ est un sous-espace vectoriel de $\mathcal{P}(\Omega)$, puis déduire l'égalité $\mathcal{B}'_\omega = \mathcal{B}_\omega$.

I.B.3.c. Déduire des questions précédentes que le polynôme des poids de $\mathcal{B}_\omega$ est :

$$Q_\omega(X,Y) = \frac{1}{2}\left(\left(X^2+Y^2\right)^m + \left(X^2-Y^2\right)^m + (2XY)^m\right).$$

I.B.3.d. On dit qu'un code auto-orthogonal est pair si les cardinaux de tous ses éléments sont multiples de 4. Vérifier que le code $\mathcal{B}_\omega$ défini ci-dessus est pair dès que ω est multiple de 8.

I.B.3.e. Si $\omega = 16$, on se propose de construire un code $\mathcal{B}''_{16}$ non isomorphe à $\mathcal{B}_{16}$ et dont le polynôme des poids est $Q_{16}(X,Y)$. On remarque que $(Q_8(X,Y))^2 = Q_{16}(X,Y)$. Si :

$$\Omega = \{t_1, t_2, ..., t_8, u_1, u_2, ..., u_8\},$$

on note $\Omega' = \{t_1, t_2, t_3, t_4, u_1, u_2, u_3, u_4\}$ et $\Omega'' = \{t_5, t_6, t_7, t_8, u_5, u_6, u_7, u_8\}$. Soit $\mathcal{C}'$ (resp. $\mathcal{C}''$) un code de Ω' (resp. Ω'') du même type que $\mathcal{B}_8$. On construit le code :

$$\mathcal{B}''_{16} = \mathcal{C}' + \mathcal{C}'' = \left\{x' + x'' \,/\, x' \in \mathcal{C}' \text{ et } x'' \in \mathcal{C}''\right\}$$

de $\mathcal{P}(\Omega)$. Calculer le polynôme des poids Q''_{16} de $\mathcal{B}''_{16}$. On pose :

$$\begin{cases} x = \{t_1, t_2, t_3, t_4\} \\ \mathcal{E} = \{y \in \mathcal{B}_{16} \,/\, |y| = 4 \text{ et } |x \cap y| = 2\} \\ \mathcal{E}'' = \{y \in \mathcal{B}''_{16} \,/\, |y| = 4 \text{ et } |x \cap y| = 2\}. \end{cases}$$

Montrer que $\bigcup_{y\in\mathcal{E}} y = \Omega$, puis que $\bigcup_{y\in\mathcal{E}''} y = \Omega'$. On admettra que ces égalités sont encore vraies si l'on remplace $x = \{t_1, t_2, t_3, t_4\}$ par n'importe quelle partie x de cardinal 4 de Ω et si l'on prend soin de conclure à $\bigcup_{y\in\mathcal{E}''} y = \Omega'$ ou à $\bigcup_{y\in\mathcal{E}''} y = \Omega''$ cette fois-ci. Expliquer brièvement pourquoi $\mathcal{B}''_{16}$ et $\mathcal{B}_{16}$ ne sont pas isomorphes.

I.B.4. Soit $\mathcal{C}$ un code de $\mathcal{P}(\Omega)$. On se propose de démontrer l'identité de Mac Williams (1963) :

$$2^{\dim\mathcal{C}} \times P_{\mathcal{C}^\perp}(X,Y) = P_{\mathcal{C}}(Y-X, X+Y). \quad \textbf{(MW)}$$

I.B.4.a. Soit $f : \mathcal{P}(\Omega) \to M$ une application à valeurs dans un groupe abélien M dont la loi est notée additivement.
On pose $(-1)^{\overline{0}} = 1$ et $(-1)^{\overline{1}} = -1$, et l'on note $\widehat{f} : \mathcal{P}(\Omega) \to M$ la fonction définie par :

$$\widehat{f}(x) = \sum_{y\in\mathcal{P}(\Omega)} (-1)^{\alpha(x,y)} f(y).$$

Démontrer que pour tout code $\mathcal{C}$ de $\mathcal{P}(\Omega)$, on a :

$$\sum_{x\in\mathcal{C}} \widehat{f}(x) = 2^{\dim\mathcal{C}} \sum_{y\in\mathcal{C}^\perp} f(y).$$

I.B.4.b. Ecrire la formule de la question précédente avec $M = \mathbb{Z}[X,Y]$ et :

$$\begin{array}{rccc} f: & \mathcal{P}(\Omega) & \to & \mathbb{Z}[X,Y] \\ & x & \mapsto & X^{|x|}Y^{\omega-|x|}. \end{array}$$

Montrer ensuite que l'identité de Mac Williams sera bien démontrée si l'on prouve que :

$$\widehat{f}(x) = (Y-X)^{|x|}(X+Y)^{\omega-|x|}$$

pour tout $x \in \mathcal{C}$. Démontrer cette dernière formule (Indication : Dans l'expression sommatoire donnant $\widehat{f}$, on pourra écrire toute partie y de $\mathcal{P}(\Omega)$ sous la forme $y = y_1 + y_2$ avec $y_1 \subset x$ et $y_2 \subset \Omega\backslash x$).

Partie II

II.A. Invariants d'un groupe fini

Soit V un espace vectoriel de dimension finie $n \geq 1$ sur le corps des complexes $\mathbb{C}$. Si g est un endomorphisme de V, on note $\mathrm{Tr}(g)$ sa trace. On note Id l'endomorphisme identité sur V, $\mathrm{Aut}(V)$ le groupe des automorphismes de V, et G un sous-groupe fini de $\mathrm{Aut}(V)$.

II.A.1. Soit V^G le sous-espace vectoriel de V formé des vecteurs v tels que $g(v) = v$ pour tout $g \in G$. Soit p_G l'endomorphisme de V défini par :

$$p_G = \frac{1}{|G|}\sum_{g\in G} g.$$

II.A.1.a. Montrer que $\mathrm{Im}(p_G) = V^G$ et que p_G est un projecteur de V.

II.A.1.b. En déduire la formule :

$$\dim\left(V^G\right) = \frac{1}{|G|}\sum_{g\in G} \mathrm{Tr}(g).$$

II.A.1.c. Si G' est un groupe fini quelconque et si $\varphi : G' \to \mathrm{Aut}(V)$ est un morphisme de groupes, on pose :

$$V^{G'} = \left\{v \in V \,/\, \forall g' \in G' \quad \varphi\left(g'\right)(v) = v\right\}.$$

Démontrer la formule plus générale :

$$\dim(V^{G'}) = \frac{1}{|G'|} \sum_{g' \in G'} \mathrm{Tr}\left(\varphi\left(g'\right)\right).$$

II.A.2. On choisit une base $e = (e_1, ..., e_n)$ de V, et l'on note A l'algèbre $\mathbb{C}[X_1, ..., X_n]$ des polynômes d'indéterminées X_1, ..., X_n et à coefficients dans $\mathbb{C}$. A tout élément g de $\mathrm{Aut}(V)$ on associe l'application $\sigma_g : A \to A$ définie de la manière suivante :
Si $g(e_h) = \sum_{j=1}^{n} \gamma_{jh} e_j$ pour tout $h \in \mathbb{N}_n$, et si $P(X_1, ..., X_n) \in A$, alors :

$$\sigma_g(P)(X_1, ..., X_n) = P\left(\sum_{j=1}^{n} \gamma_{j1} X_j, ..., \sum_{j=1}^{n} \gamma_{jn} X_j\right).$$

II.A.2.a. Montrer que σ_g est un automorphisme de l'algèbre A, et que l'application :

$$\begin{array}{cccc} \Psi : & \mathrm{Aut}(A) & \to & \mathrm{Aut}(A) \\ & g & \mapsto & \sigma_g \end{array}$$

est un homomorphisme de groupes.

II.A.2.b. Soit A_k $(k \in \mathbb{N})$ le sous-espace vectoriel de A formé des polynômes homogènes de degré k. Quelle est la dimension a_k de A_k ? Vérifier que $\sigma_g(A_k) = A_k$ pour tout g appartenant à $\mathrm{Aut}(A)$. On notera $g_k = \sigma_g|_{A_k}$ la restriction de σ_g à A_k, et l'on dira que g_k est l'automorphisme de A_k définie par g.

II.A.3. On pose :

$$A_k^G = \{P \in A_k \,/\, \forall g \in G \quad \sigma_g(P) = P\}$$

et $a_k(G) = \dim\left(A_k^G\right)$. Démontrer que les deux séries entières $\sum_{k=0}^{+\infty} a_k z^k$ et $\sum_{k=0}^{+\infty} a_k(G) z^k$ ont des rayons de convergence strictement positifs.

II.A.4. Soit $g \in G$. On pose :

$$\Phi_G(z) = \sum_{k=0}^{+\infty} a_k(G) z^k \quad \text{et} \quad \frac{1}{\det(Id - zg)} = \sum_{k=0}^{+\infty} r_k z^k.$$

II.A.4.a. Montrer que la série entière $\sum_{k=0}^{+\infty} r_k z^k$ possède un rayon de convergence ≥ 1.

II.A.4.b. On suppose que la matrice de g dans la base e est diagonale et on la note $\mathrm{diag}(\alpha_1, ..., \alpha_n)$. Exprimer r_k en fonction des complexes $\alpha_1, ..., \alpha_n$ et de l'entier k. En déduire l'égalité $\mathrm{Tr}(g_k) = r_k$.

II.A.4.c. On se place maintenant dans le cas général où $g \in G$. Montrer que g est diagonalisable, et en déduire l'égalité $\mathrm{Tr}(g_k) = r_k$.

II.A.4.d. Utiliser les questions **II.A.1.c.** et **II.A.4.c.** pour montrer l'égalité :

$$\Phi_G(z) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(Id - zg)}.$$

pour tout z tel que $|z| < 1$.

II.B. Algèbre associée aux polynômes des poids

On utilise les notations, définitions et résultats des parties I.A, I.B et II.A. On note G le groupe des matrices engendrées par :

$$\mu = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{et} \quad \rho = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Si $P(X,Y) \in \mathbb{C}[X,Y]$ et si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, on rappelle que (cf. II.A) :

$$\sigma_g(P)(X,Y) = P(aX + cY, bX + dY).$$

II.B.1. Soit $\mathcal{C}$ un code auto-orthogonal de $\mathcal{P}(\Omega)$. On rappelle qu'alors $\dim \mathcal{C} = \omega/2$ et que tous les mots de $\mathcal{C}$ sont de cardinal pair. En utilisant la formule de Mac Williams **(MW)**, démontrer que $P_{\mathcal{C}}(X,Y)$ est invariant par les transformations lorsque $g \in G$.

II.B.2. Quelle est la nature géométrique de l'endomorphisme μ ? Et celle de ρ ? En déduire la nature de la composée $\rho\mu$ puis l'ordre du groupe monogène H engendré par $\rho\mu$. Montrer que H est un sous-groupe distingué de G. Expliciter le quotient G/H, puis en déduire le cardinal de G.

On pose $A = \mathbb{C}[X,Y]$ et on utilise les notations de II.A pour $n = 2$.

II.B.3.a. Décomposer la fraction rationnelle :

$$\frac{1}{(1-X^2)(1-X^8)}$$

en éléments simples dans $\mathbb{R}(X)$.

II.B.3.b. Calculer le déterminant $\det(Id - zg)$ lorsque g est une réflexion ou une rotation de l'espace euclidien $\mathbb{R}^2$. En utilisant **II.A.4.d**, en déduire que :

$$\Phi_G(z) = \frac{1}{(1-z^2)(1-z^8)}.$$

pour tout complexe z tel que $|z| < 1$.

II.B.4. Si r est un réel, on note $[r]$ sa partie entière. En utilisant les question **II.A.4** et **II.B.3.b** montrer que la dimension $a_k(G)$ de l'espace A_k^G des polynômes homogènes à deux variables de degré k invariants par G est :

$$a_k(G) = \begin{cases} [k/8] + 1 \text{ si } k \text{ est pair,} \\ 0 \text{ si } k \text{ est impair.} \end{cases}$$

II.B.5. On considère l'algèbre :

$$\begin{aligned} A' &= \mathbb{C}[P_2(X,Y), Q_8(X,Y)] \\ &= \{P(P_2(X,Y), Q_8(X,Y)) \,/\, P(X,Y) \in \mathbb{C}[X,Y]\} \end{aligned}$$

engendrée par les polynômes $P_2(X,Y) = X^2 + Y^2$ et :

$$Q_8(X,Y) = \frac{1}{2}\left(\left(X^2+Y^2\right)^4 + \left(X^2-Y^2\right)^4 + (2XY)^4\right).$$

On note A'_k la composante homogène de A' de degré k. En remarquant que les polynômes P_2 et Q_8 ont déjà été introduits en **I.B.2** et **I.B.3**, démontrer les inclusions $A' \subset A^G$ et $A'_k \subset A_k^G$.

Comme P_2 et Q_8 sont homogènes de degré 2 et 8, la composante homogène A'_k sera engendré par la famille :

$$\left\{P_2^i Q_8^j\right\}_{(i,j)\in\mathbb{N}\times\mathbb{N} \text{ et } 2i+8j=k}.$$

Démontrer que cette famille est libre, et en déduire l'égalité $A' = A^G$.

II.B.6. On pose $\Delta(X,Y) = X^2Y^2\left(X^2 - Y^2\right)^2$ et l'on remarque que :

$$Q_8 = P_2^4 - 4\Delta.$$

Démontrer que si $\mathcal{C}$ est un code auto-orthogonal de $\mathcal{P}(\Omega)$, le polynôme $P_{\mathcal{C}}(X,Y)$ appartient à l'algèbre :

$$\mathbb{Z}\left[P_2(X,Y), \Delta(X,Y)\right] = \left\{P\left(P_2(X,Y), \Delta(X,Y)\right) / P(X,Y) \in \mathbb{Z}[X,Y]\right\}.$$

Partie III

Dans cette partie on considère l'espace vectoriel $\mathbb{Q}^\omega$ muni du produit scalaire canonique défini par :

$$(v,w) \mapsto v.w = v_1.w_1 + ... + v_\omega.w_\omega \in \mathbb{Q}.$$

lorsque $v = (v_1, ..., v_\omega)$ et $w = (w_1, ..., w_\omega)$. On dit qu'un sous-groupe additif L de $\mathbb{Q}^\omega$ est un réseau de $\mathbb{Q}^\omega$ s'il existe une base $e = (e_1, ..., e_\omega)$ de $\mathbb{Q}^\omega$ pour laquelle L est l'ensemble de toutes les combinaisons linéaires à coefficients entiers relatifs des vecteurs $e_1, ..., e_\omega$. Dans ce cas, on note $L = \mathbb{Z}e_1 + ... + \mathbb{Z}e_\omega$ et l'on dit que e est une $\mathbb{Z}$-base de L.

III.A. Généralités sur les réseaux

III.A.1. Soit L un réseau de $\mathbb{Q}^\omega$. On appelle dual de L, et on note L^0, l'ensemble des vecteurs $v \in \mathbb{Q}^\omega$ tels que $v.w \in \mathbb{Z}$ pour tout $w \in L$. Démontrer que le dual d'un réseau est un réseau.

III.A.2. Soit L un réseau de $\mathbb{Q}^\omega$ et $e = (e_1, ..., e_\omega)$ une $\mathbb{Z}$-base de L. On considère une famille $e' = (e'_1, ..., e'_\omega)$ de ω vecteurs dans L, et l'on note $P_e^{e'}$ la matrice carrée de taille ω dont les colonnes sont formées des coordonnées des vecteurs e'_j dans la base e.

III.A.2.a. Montrer que le système e' est une $\mathbb{Z}$-base de L si et seulement si $\det(P_e^{e'}) = \pm 1$.

III.A.2.b. En déduire que la valeur absolue du déterminant d'une $\mathbb{Z}$-base de L par rapport à une base orthonormale de $\mathbb{Q}^\omega$ ne dépend que de L. Cette valeur est appelée volume de L et notée $\mathrm{Vol}(L)$.

III.A.2.c. Démontrer que $\mathrm{Vol}(L)\,\mathrm{Vol}\left(L^0\right) = 1$.

III.A.3. Dans cette question, M désigne un sous-groupe additif de $\mathbb{Q}^\omega$ engendré par un nombre fini d'éléments e'_1, ..., e'_s de $\mathbb{Q}^\omega$.

III.A.3.a. Montrer l'existence d'au moins un réseau L qui contient M.

III.A.3.b. Soit $(e_1, ..., e_\omega)$ une $\mathbb{Z}$-base de L. Pour tout $k \in \mathbb{N}_\omega$ on appelle L_k le sous-groupe additif engendré par $e_1, ..., e_k$. Démontrer par récurrence sur k que $M \cap L_k$ est engendré par k vecteurs de $\mathbb{Q}^\omega$. En déduire que le groupe M est engendré par ω vecteurs.

III.A.3.c. Déduire de la question précédente que, si M contient un réseau de $\mathbb{Q}^\omega$, alors M est lui même un réseau de $\mathbb{Q}^\omega$.

III.A.4. On suppose que ω est un multiple de 4. Soit $(w_1, ..., w_\omega)$ une base orthogonale

de $\mathbb{Q}^\omega$ telle que pour tout $j \in \{1, ..., \omega\}$ on a $w_i.w_j = 1/4$. Soit Λ_ω l'ensemble des vecteurs $v = \sum_{1 \leq j \leq \omega} \lambda_j w_j$ tels que :

(a) les λ_j sont entiers et tous de même parité,

(b) $\sum_{1 \leq j \leq \omega} \lambda_j$ est multiple de 4.

Démontrer que Λ_ω est un réseau de $\mathbb{Q}^\omega$, et que $\Lambda_\omega^0 = \Lambda_\omega$.

III.A.5. Soit L un réseau de $\mathbb{Q}^\omega$. Démontrer qu'il existe un entier $d \geq 1$ tel que $L \subset \frac{1}{d}\mathbb{Z}^\omega$, puis que l'on peut définir l'entier :

$$d_L = \text{Min}\left\{m \in \mathbb{N}^* \,/\, m \left\|v\right\|^2 \in \mathbb{N}\right\}.$$

Pour tout entier naturel k, on note $c_k(L)$ le nombre de vecteurs de L de carré scalaire k/d_L. Démontrer l'inégalité :

$$c_k(L) \leq \left(2d\sqrt{\frac{k}{d_L}} + 1\right)^\omega,$$

puis en déduire que la série $\sum_{k=0}^{+\infty} c_k(L)\, e^{ik\pi z}$ est absolument convergente lorsque z appartient au demi-plan supérieur ouvert du plan de Cauchy.

On pose :

$$\theta_L(z) = \sum_{k=0}^{+\infty} c_k(L)\, e^{ik\pi z/d_L}.$$

Comme la série est commutativement et associativement convergente, on peut aussi écrire :

$$\theta_L(z) = \sum_{v \in L} e^{i(v.v)\pi z}.$$

III.B. Codes et réseaux

III.B.1. Démontrer qu'il existe une base orthogonale $(v_1, ..., v_\omega)$ de $\mathbb{Q}^\omega$ telle que l'on ait $v_i.v_i = 1/2$ pour tout $j \in \{1, ..., \omega\}$. Dans la suite du problème, on choisit une telle base et on désigne par R le réseau qu'elle engendre.

III.B.2. Dans cette question, on se propose de montrer que les $\mathbb{Z}$-bases orthogonales de R ont toutes le même ensemble image par la surjection canonique de R sur $R/2R$.

III.B.2.a. Soit $v' = (v_1', ..., v_\omega')$ une base orthogonale de $\mathbb{Q}^\omega$. On note $P_e^{v'}$ la matrice de passage de la base canonique e vers la base v'. Calculer la matrice ${}^t(P_e^{v'})P_e^{v'}$ et en déduire la formule :

$$(\det P_e^{v'})^2 = \prod_{j=1}^{\omega} \left(v_j'.v_j'\right).$$

III.B.2.b. Calculer $(\text{Vol}\,(R))^2$. En déduire que, si $v' = (v_1', ..., v_\omega')$ désigne une $\mathbb{Z}$-base orthogonale de R, alors :

$$\prod_{j=1}^{\omega} \left(v_j'.v_j'\right) = \frac{1}{2^\omega}.$$

Utiliser cette relation pour montrer qu'il existe des entiers ε_j $(1 \leq j \leq \omega)$.valant ± 1 et tels que $\{v_1', ..., v_\omega'\} = \{\varepsilon_1 v_1, ..., \varepsilon_\omega v_\omega\}$. Conclure.

III.B.3. On note Ω l'ensemble image d'une $\mathbb{Z}$-base orthogonale de R dans $R/2R$. On désigne par $\overline{v}$ l'image de v dans $R/2R$. Le groupe-quotient $R/2R$ est muni d'une structure naturelle d'espace vectoriel sur le corps à deux éléments $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. On munit cet espace de la forme bilinéaire symétrique β définie par $\beta(\overline{v}, \overline{w}) = \overline{2v.w}$.
Vérifier que l'espace vectoriel $R/2R$ muni de la forme bilinéaire β est canoniquement isomorphe à $\mathcal{P}(\Omega)$ muni de la forme bilinéaire naturelle α. On identifiera dorénavant $R/2R$ et $\mathcal{P}(\Omega)$.

III.B.4. Soit $\mathcal{C}$ un code de $\mathcal{P}(\Omega)$. On note $L(\mathcal{C})$ l'image réciproque de $\mathcal{C}$ par la surjection canonique de R sur $R/2R = \mathcal{P}(\Omega)$.

III.B.4.a. Montrer que $2R \subset L(\mathcal{C}) \subset R$. Utiliser la question **III.A.3** pour démontrer que $L(\mathcal{C})$ est un réseau.

III.B.4.b. Montrer que $(2R)^0 = R$. En déduire $L(\mathcal{C})^0 \subset R$ puis que $L(\mathcal{C})^0 = L(\mathcal{C}^0)$.

III.B.4.c. Soit $(u_1, ..., u_\omega)$ une $\mathbb{Z}$-base de $L(\mathcal{C})$. Expliquer pourquoi le système $(\overline{u}_1, ..., \overline{u}_\omega)$ engendre l'espace vectoriel $\mathcal{C}$. On pose $d = \dim \mathcal{C}$, et l'on suppose que $(\overline{u}_1, ..., \overline{u}_d)$ est une base de $\mathcal{C}$ quitte à modifier l'ordre des vecteurs. Soit X le sous-groupe engendré par les vecteurs $u_1, ..., u_d$. Montrer que pour tout $j \geq d+1$ il existe $x_j \in X$ tel que $u'_j = u_j - x_j \in 2R$.

III.B.4.d. On conserve les notations de la question précédente. Démontrer que :

$$\left(u_1, ..., u_d, u'_{d+1}, ..., u'_\omega\right)$$

est une $\mathbb{Z}$-base de $L(\mathcal{C})$, puis que $\left(2u_1, ..., 2u_d, u'_{d+1}, ..., u'_\omega\right)$ est une $\mathbb{Z}$-base de $2R$. En utilisant la question **III.B.2.b**, déduire alors l'égalité :

$$\mathrm{Vol}\,(L(\mathcal{C})) = 2^{\frac{\omega}{2} - \dim(\mathcal{C})}.$$

III.B.5. Dans cette question on montre que $P_{\mathcal{C}}(\varphi_2(z), \varphi_3(z)) = \theta_{L(\mathcal{C})}(z)$.

III.B.5.a. Montrer que les séries :

$$\sum_{k=0}^{+\infty} e^{i2\pi\left(k+\frac{1}{2}\right)^2 z} \quad \text{et} \quad \sum_{k=0}^{+\infty} e^{i2\pi k^2 z}$$

convergent pour tout z appartenant au demi-plan ouvert supérieur du plan de Cauchy.

III.B.5.b. En notant que l'on peut écrire :

$$\varphi_2(z) = \sum_{\substack{m \text{ impair} \\ m \in \mathbb{Z}}} e^{i\pi \frac{m^2}{2} z} \text{ et } \varphi_3(z) = \sum_{\substack{m \text{ pair} \\ m \in \mathbb{Z}}} e^{i\pi \frac{m^2}{2} z},$$

montrer que :

$$P_{\mathcal{C}}(\varphi_2(z), \varphi_3(z)) = \sum_{h=0}^{+\infty} v_h e^{i\pi \frac{h}{2} z}$$

où $v_h = \sum_{x \in \mathcal{C}} \Theta_x$, en notant Θ_x le cardinal de l'ensemble des :

$$\left(m_1, ..., m_{|x|}, n_1, ..., n_{\omega-|x|}\right) \in \mathbb{Z}^\omega$$

tels que :

$$\begin{cases} m_j \text{ impair et } n_j \text{ pair,} \\ m_1^2 + ... + m_{|x|}^2 + n_1^2 + ... + n_{\omega-|x|}^2 = h. \end{cases}$$

III.B.5.c. Montrer que $\theta_{L(\mathcal{C})}(z) = \sum_{h=0}^{+\infty} d_h e^{i\pi \frac{h}{2} z}$ où :

$$\Lambda_h = \left\{ v \in L(\mathcal{C}) \;/\; v.v = \frac{h}{2} \right\}$$

et $d_h = |\Lambda_h|$.

III.B.5.d. En écrivant l'ensemble Λ_h comme la réunion disjointe :

$$\Lambda_h = \bigcup_{x \in \mathcal{C}} \Lambda_{h,x} \quad \text{où } \Lambda_{h,x} = \left\{ v \in L(\mathcal{C}) \;/\; \overline{v} = x \text{ et } v.v = \frac{h}{2} \right\},$$

montrer que $d_h = v_h$. Conclure.

Avertissement – L'énoncé proposé ici a été légèrement modifié par rapport à celui de la composition de mathématiques générales de l'agrégation externe 1978. Tout d'abord j'ai supprimé les deux questions originelles III.B.5 et III.B.6 de la dernière partie, que je considère comme purement techniques et assez gratuites. Ensuite j'ai fractionné et détaillé un certain nombre de questions que j'ai jugées trop abruptes, dans le but de rendre le problème plus abordable et formateur.